PROFESSIONAL-CLOUD-SECURITY-ENGINEER$^{Q\&As}$

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Correct Answer: BC

https://cloud.google.com/vpc/docs/vpc-peering#key_properties

QUESTION 2

Your organization\\'s Google Cloud VMs are deployed via an instance template that configures them with a public IP address in order to host web services for external users. The VMs reside in a service project that is attached to a host (VPC) project containing one custom Shared VPC for the VMs. You have been asked to reduce the exposure of the VMs to the internet while continuing to service external users. You have already recreated the instance template without a public IP address configuration to launch the managed instance group (MIG). What should you do?

A. Deploy a Cloud NAT Gateway in the service project for the MIG.

B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.

C. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.

D. Deploy an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.

Correct Answer: C

QUESTION 3

Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer.

What type of Load Balancing should you use?

A. Network Load Balancing

B. HTTP(S) Load Balancing

C. TCP Proxy Load Balancing

D. SSL Proxy Load Balancing

Correct Answer: D

https://cloud.google.com/load-balancing/docs/ssl -SSL Proxy Load Balancing is a reverse proxy load balancer that distributes SSL traffic coming from the internet to virtual machine (VM) instances in your Google Cloud VPC network. https://cloud.google.com/load-balancing/docs/ssl/

QUESTION 4

Your company uses Google Cloud and has publicly exposed network assets. You want to discover the assets and perform a security audit on these assets by using a software tool in the least amount of time.

What should you do?

A. Run a platform security scanner on all instances in the organization.

B. Notify Google about the pending audit and wait for confirmation before performing the scan.

C. Contact a Google approved security vendor to perform the audit.

D. Identify all external assets by using Cloud Asset Inventory and then run a network security scanner against them.

Correct Answer: D

QUESTION 5

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?

A. VPC Flow Logs

B. Cloud Armor

C. DNS Security Extensions

D. Cloud Identity-Aware Proxy

Correct Answer: C

Reference: https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns DNSSEC --use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof. Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like www.example.com into its associated IP address is an increasingly important building block of today\\'s web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites. https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns